

## **RES TechNote**

# **Parsing Remote User Access via PowerFuse and Citrix Web Interface**

### **Executive Summary**

This document describes the steps necessary to configure the RES PowerFuse Desktop for remote access via Citrix Web Interface to a specific subset of users within the network.

The customer delivers remote access to the RES PowerFuse Published Desktop via Citrix Web Interface. The customer has an internal network of thin client devices accessing the RES PowerFuse Published Desktop, and wants to manage a single desktop application instance for both task workers and managers. But, the customer wants managers to have remote access to the RES PowerFuse Published Desktop via the Citrix Web Interface.

Citrix Web Interface is capable of delivering secure remote access to end users via SSL encryption. Unfortunately however, Citrix Web Interface lacks the ability to meet the customer's requirement of delivering remote access to a subset of users, while these same applications are available to all users internally from a single published application within the Citrix farm environment.

### **Prerequisites:**

In order to get the most out of this document, it is recommended that the consultant/integrator is familiar with RES PowerFuse technology and terminology. If concepts such as Workspaces, PowerZones are not familiar, it is advised to consult with a RES Certified Administrator in order to implement this in a production environment.

The information below is to be used at your own risk without exception. How you manage access to your application environment should be thoroughly tested prior to introduction to the production environment. Test these configurations thoroughly in your lab.

To configure the access control within the RES PowerFuse Management Console (PFMC), the following items will be required within the network.

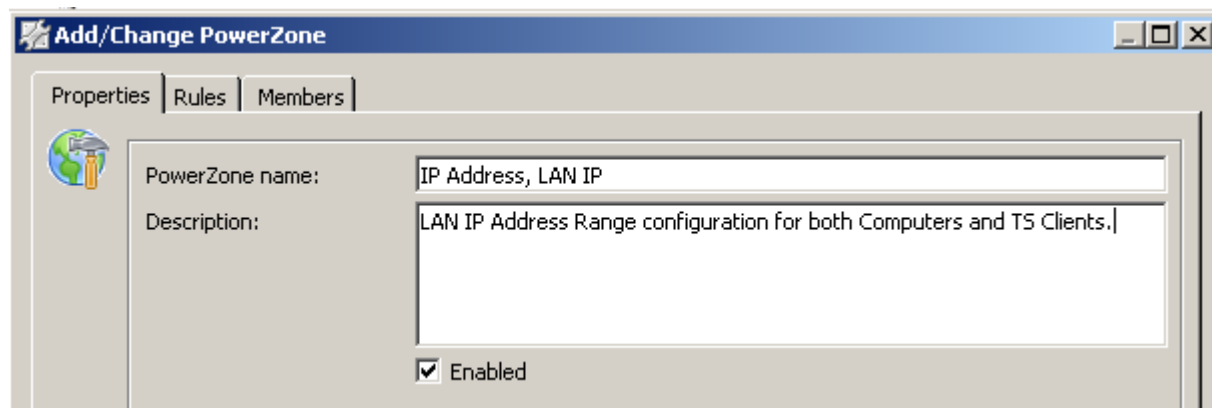
- AD User Group: Managers user group will contain all users capable of remote access to the published desktop.
- PowerZone: PowerZone configured for IP Address Range of the internal network for both Computers and TS Clients.
- Workspace Container: PowerFuse Desktop\_GlobalUsers
- Workspace Container: PowerFuse Desktop\_Managers

## What we want to accomplish specifically:

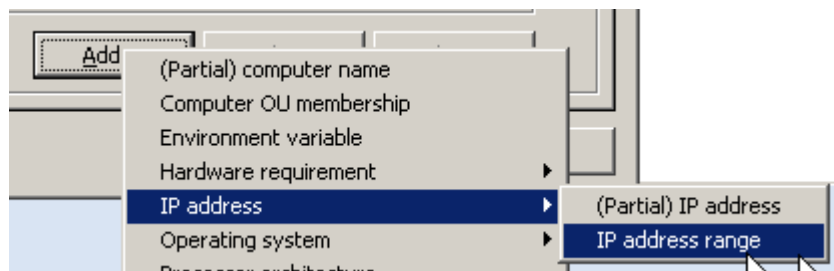
We want to configure and manage a single application configuration item for the RES PowerFuse Desktop which will be made available to all users logging onto the network internally, with only managers capable of accessing the application remotely via Citrix Web Interface.

### 1) PowerZone: Configuration:

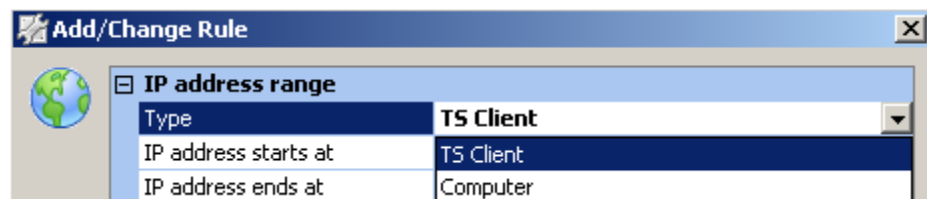
Create a PowerZone refer to the items below.

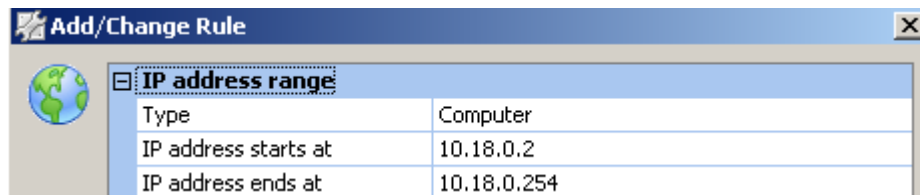
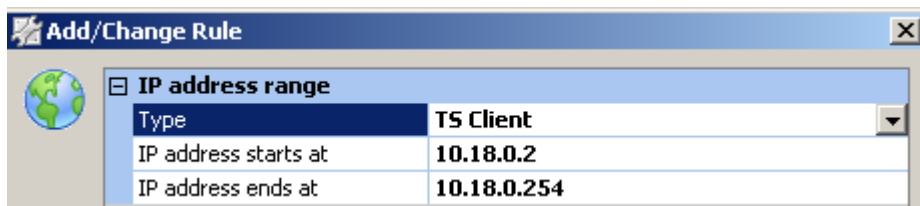


Assign the IP Address Range Rule

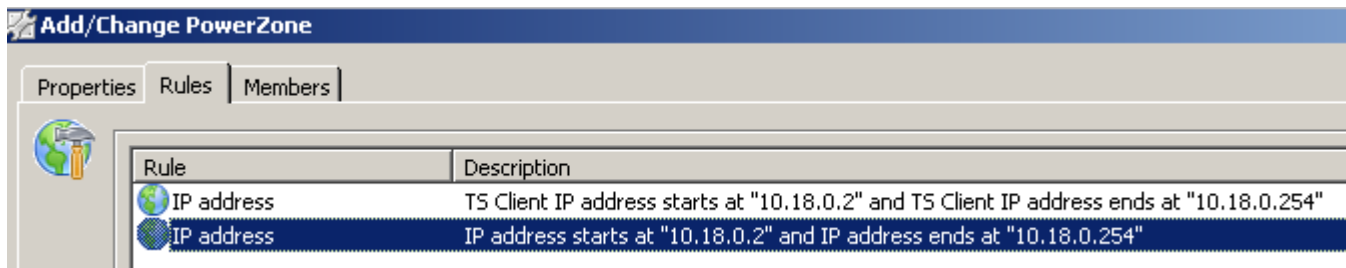


Two rules will be applied to the PowerZone, one for Computers and a second for TS Clients. Add a rule for each endpoint device option, and apply the IP address range to the rule as appropriate.





Final PowerZone rule configuration is referenced below.



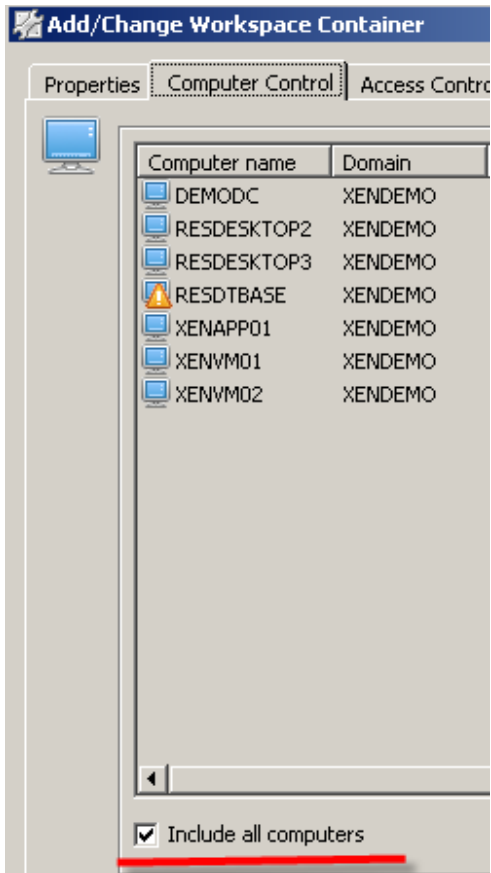
## 2) Workspace Configuration

Workspace configurations offer three means of identifying access control to network resources: Computer Control (Named Computer Accounts), Identity (OUs, Groups, and Users within AD), and Location (PowerZones defined within the PFMC). A minimum of two configuration items are required for a Workspace to be enabled within the network, Computer Control and Identity (All users is configured as default). The two Workspace configuration items are referenced below.

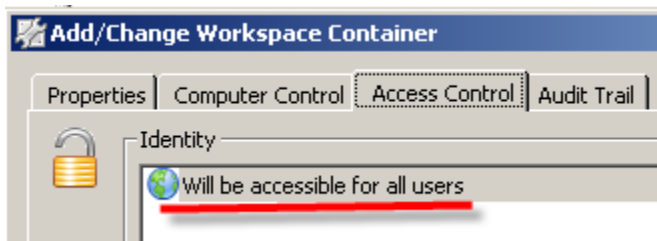
### 3) Workspace 1: PowerFuse Desktop GlobalUsers

This workspace will have three items of configuration: Computer Control (include all computers), Identity (accessible to all users), and Location (the PowerZone configured above).

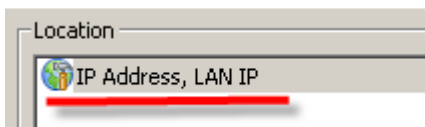
Computer Control :



Identity:



Location:



#### 4) **Workspace 2: PowerFuse Desktop Managers**

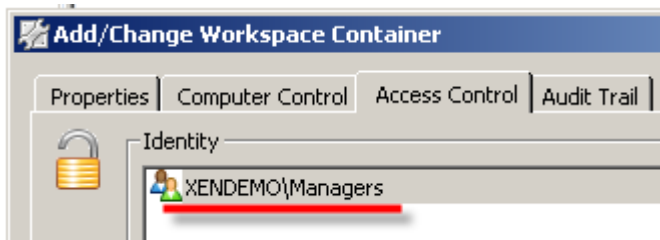
This workspace will have two items of configuration: Computer Control (Include all computers as above), Access Control (AD Group for Managers).

Computer Configuration:

Refer to the configuration referenced above.

Identity:

Apply the AD Group for Managers to the Identity configuration of the Workspace.



Location:

Location configuration for this workspace is not required.

#### 5) **Conclusion:**

Again, testing is key to this configuration. The specific detail of your networks configuration is not referenced in this information. RES is in no way responsible for the configuration and delivery of your Development, Test, Approval, or Production environment. Test, test, test, and test again.

Provided the specific detail of your network configuration can be referenced within the approach to Workspace and PowerZone configuration referenced above, it will be possible to offer only Managers the opportunity to log on remotely via Web Interface.

While both task workers and managers will have access to application icons published via Citrix Web Interface, only managers will have access to these application services. The net result is that a single instance of the RES PowerFuse Desktop is required, reducing management overhead within the Citrix farm environment.

Combine this technique with the the recommendation for control of user access to files and folders, also available from the RES PowerFuse Management console, which is referenced by my colleague Edgar van Hoeijen here, <http://resinside.blogspot.com/2009/01/access-to-files-and-folders-based-on.html> to define a complete in the building out of the building security access control while leveraging Citrix Web Interface as the sole means of remote access to the network.

Interesting to note that RES Security Alerting can also be configured to further enhance the remote access security configuration.

RTE